The Human Element in Cyber Security and Critical Infrastructure Protection: Lessons Learned

Marco Carvalho, Ph.D.
Research Scientist
mcarvalho@ihmc.us

Institute for Human and Machine Cognition
40 South Alcaniz St., Pensacola, FL 32502
https://www.ihmc.us (850) 202-4446

ihmc

FLORIDA INSTITUTE FOR HUMAN & MACHINE COGNITION

A University Affiliated Research Institute

University of West Florida

FAU FLORIDA ATLANTIC UNIVERSITY

UCF

FLORIDA INSTITUTE OF TECHNOLOGY 1958

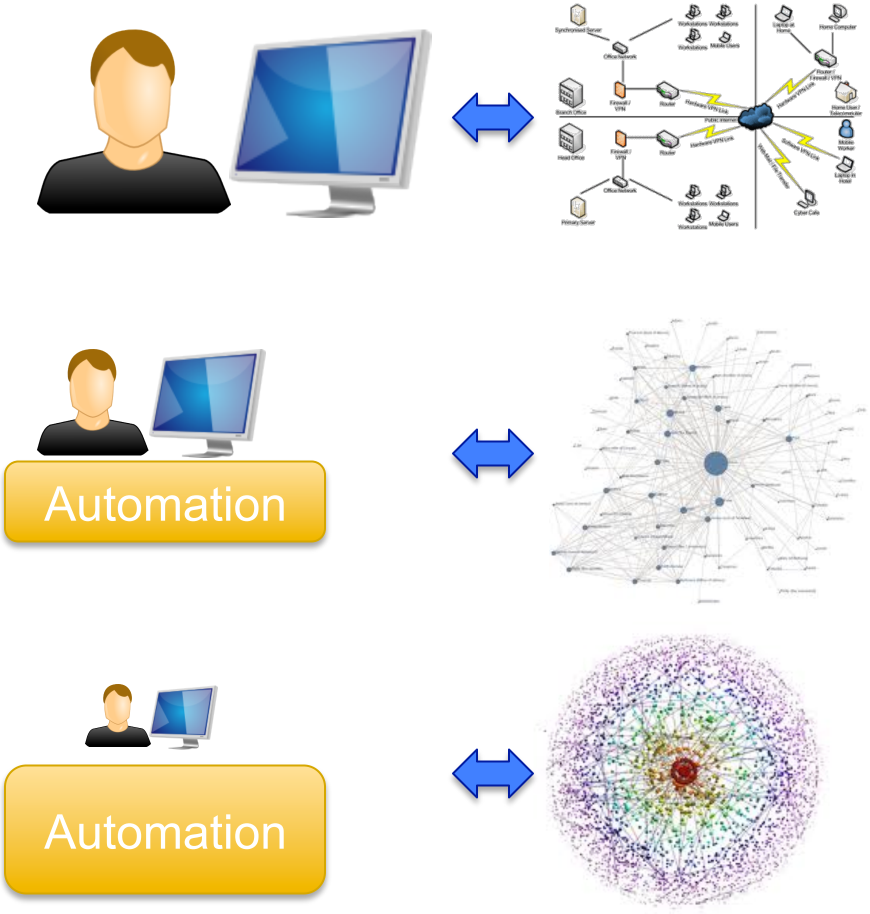
Human Centered Computing

Cyber Security and Critical Infrastructure Protection

- Complex Infrastructures
  - Multiple interacting systems
  - Often under different administrative control
  - Very large number of heterogeneous sensors and data streams
  - Multiple operating time-scales for different components and subsystems
  - Time-critical / Mission-critical
- Users generally track specific metrics at any given time.
- Difficult to model and predict

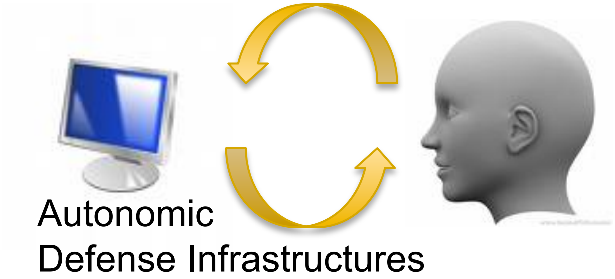
Automation in Complex System Monitoring

- Small scale systems were first monitored directly by users.
  - User has a mental model of the system
  - Single administrative domain
- Increasing scale and complexity requires some level of automation
  - High-tempo events
  - Large number of nodes
  - Large number of events
  - Complex very complex model
- Human becomes increasingly detached form the system
- Control/Defense becomes brittle and hard to understand/control


Automation

Automation

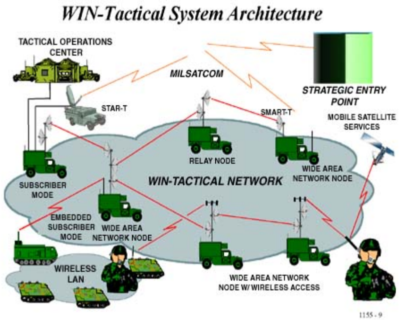
Our Research Focus: Human-Centered Defense Infrastructures



- Design security infrastructures to **enhance** human capabilities and performance on **monitoring, diagnostics and control** of complex and critical systems.
- Design new **human-in-the-loop defense infrastructures** that are semi-autonomous or autonomic in nature – a required feature for effective defense systems.
- Build cognitive, **mix-initiative systems** for cyber defense and critical infrastructure protection.

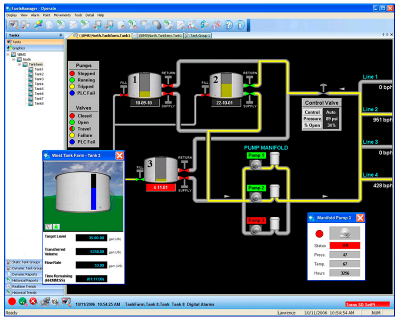
Current Projects and Lessons Learned

Enterprise Network Security



Tactical Network Security and Mission Survivability

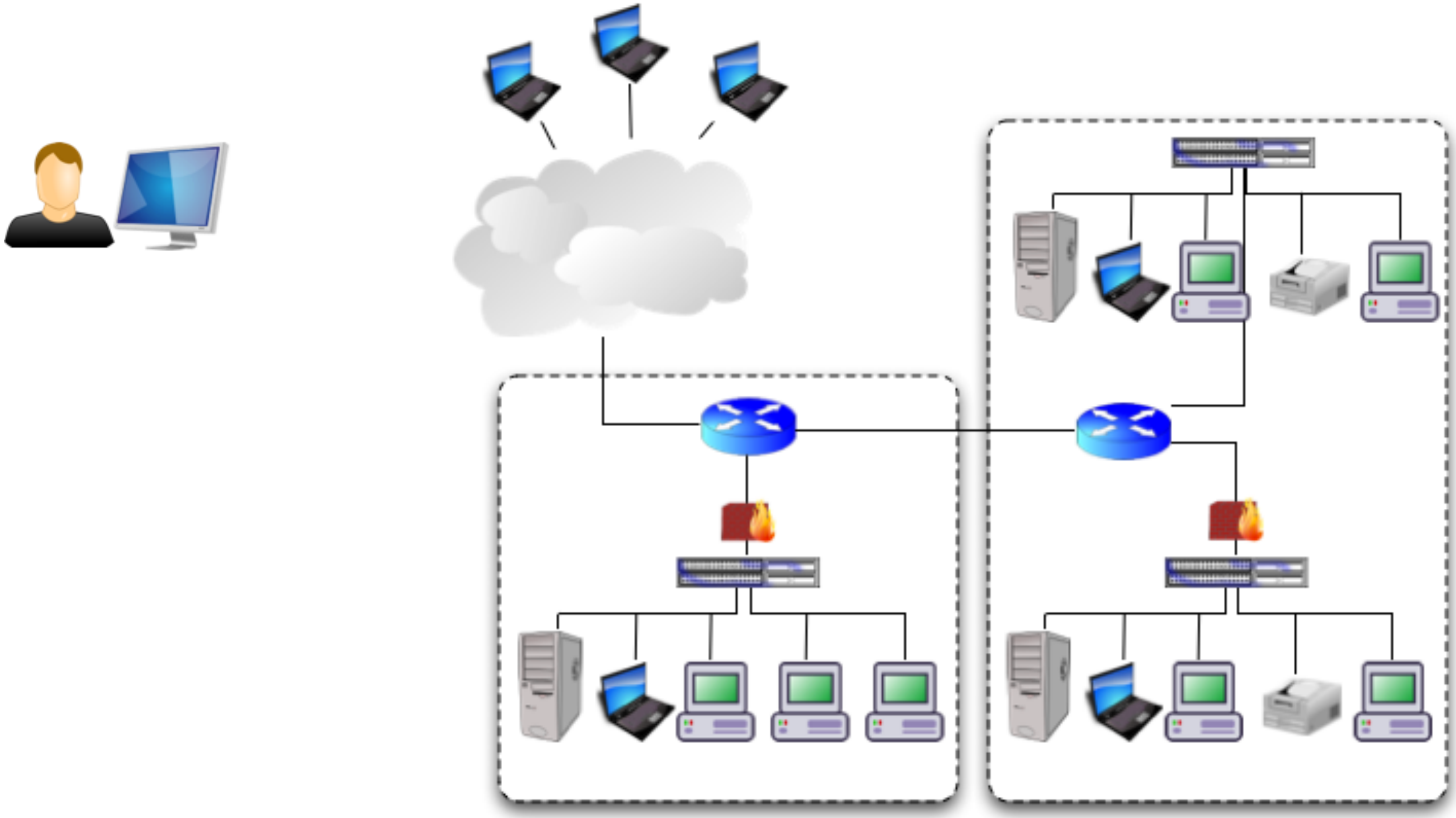
Network Operations Center



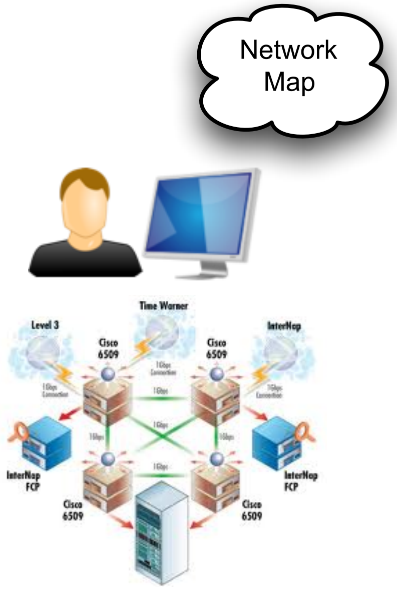
Supervisory Control and Data Acquisition – SCADA Systems

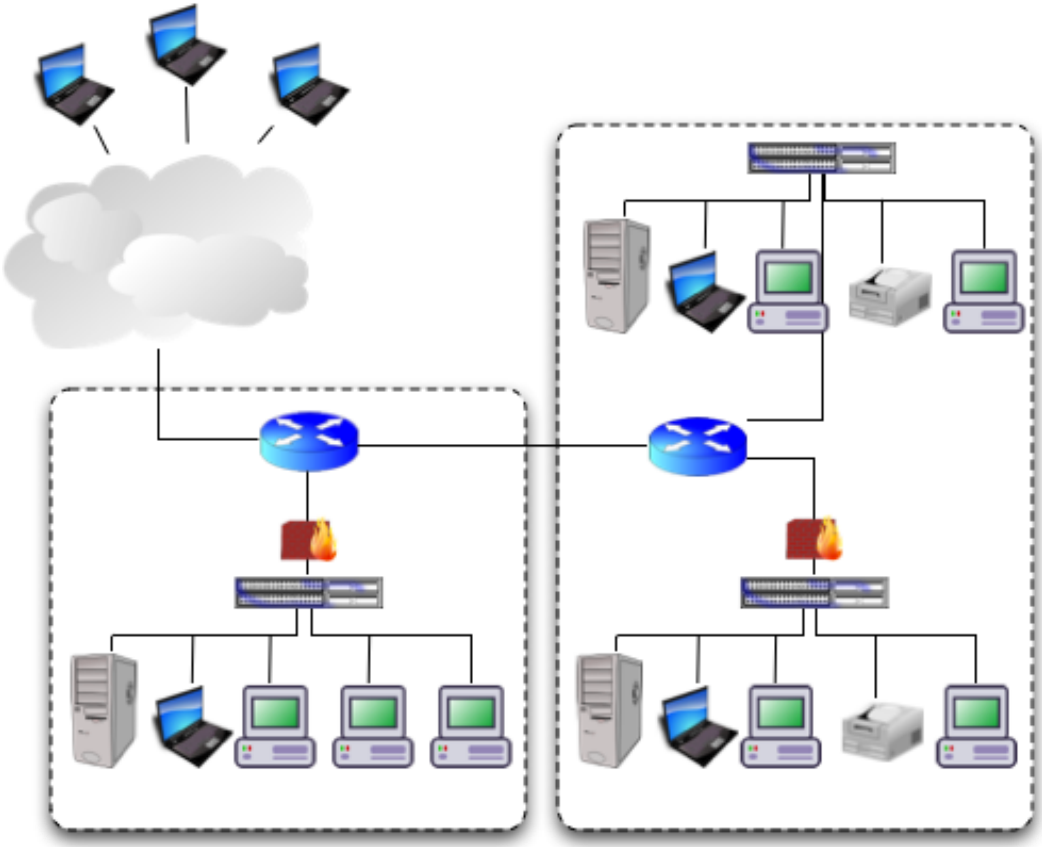
Intelligent Transportation Systems

Enterprise Network Security

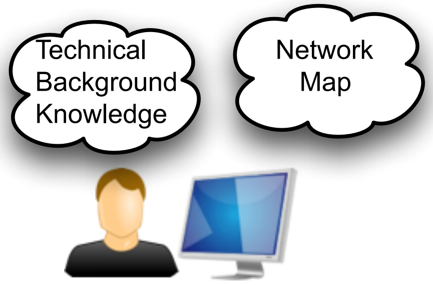


Enterprise Network Security



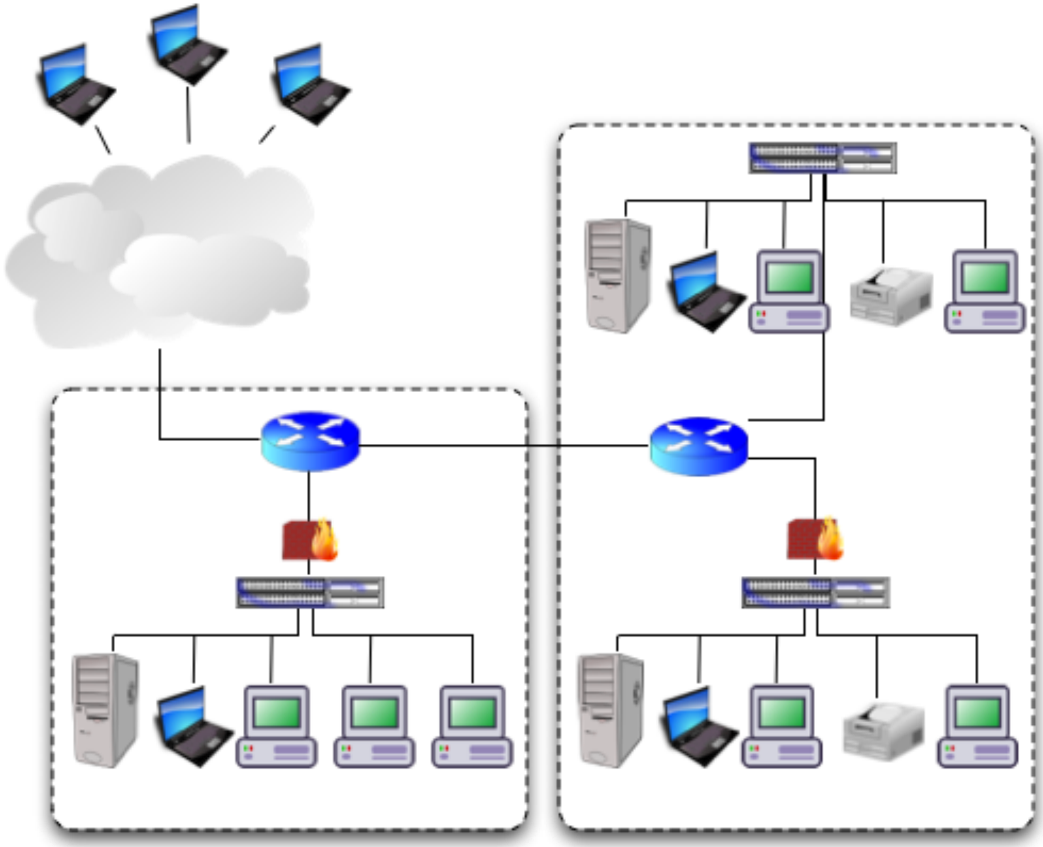


Enterprise Network Security

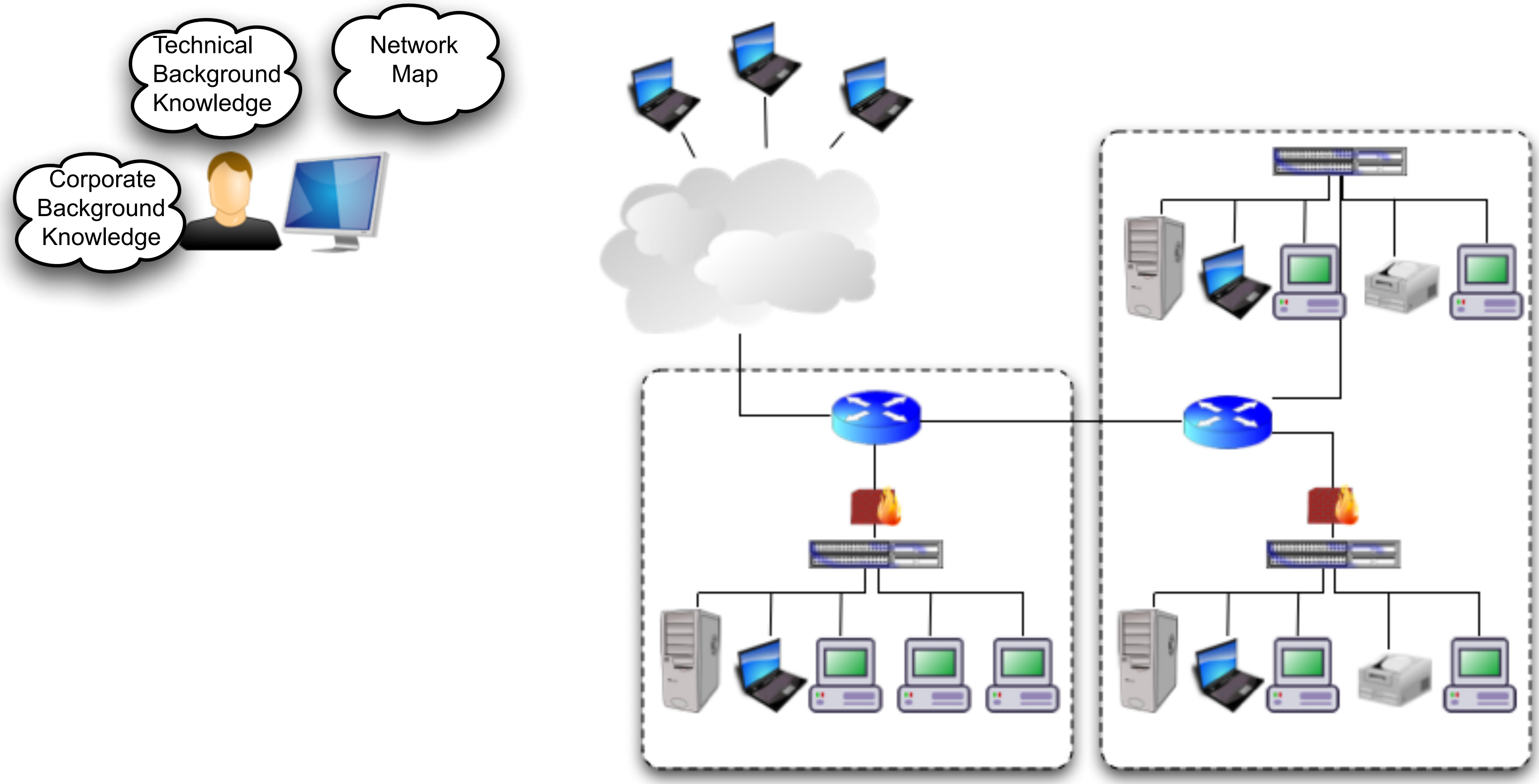


Technical Background Knowledge

Network Map



Enterprise Network Security

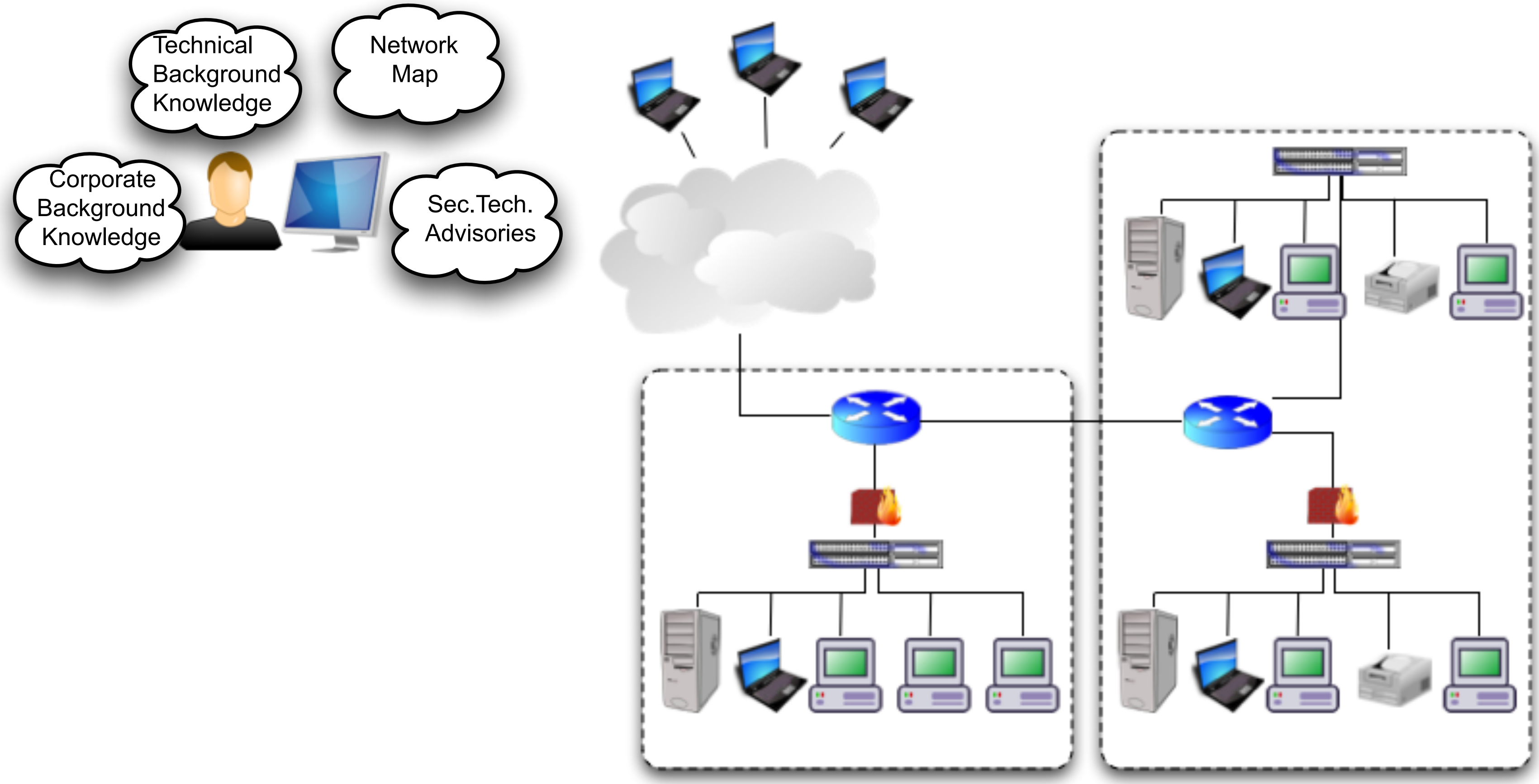


Technical Background Knowledge

Network Map

Corporate Background Knowledge

Enterprise Network Security



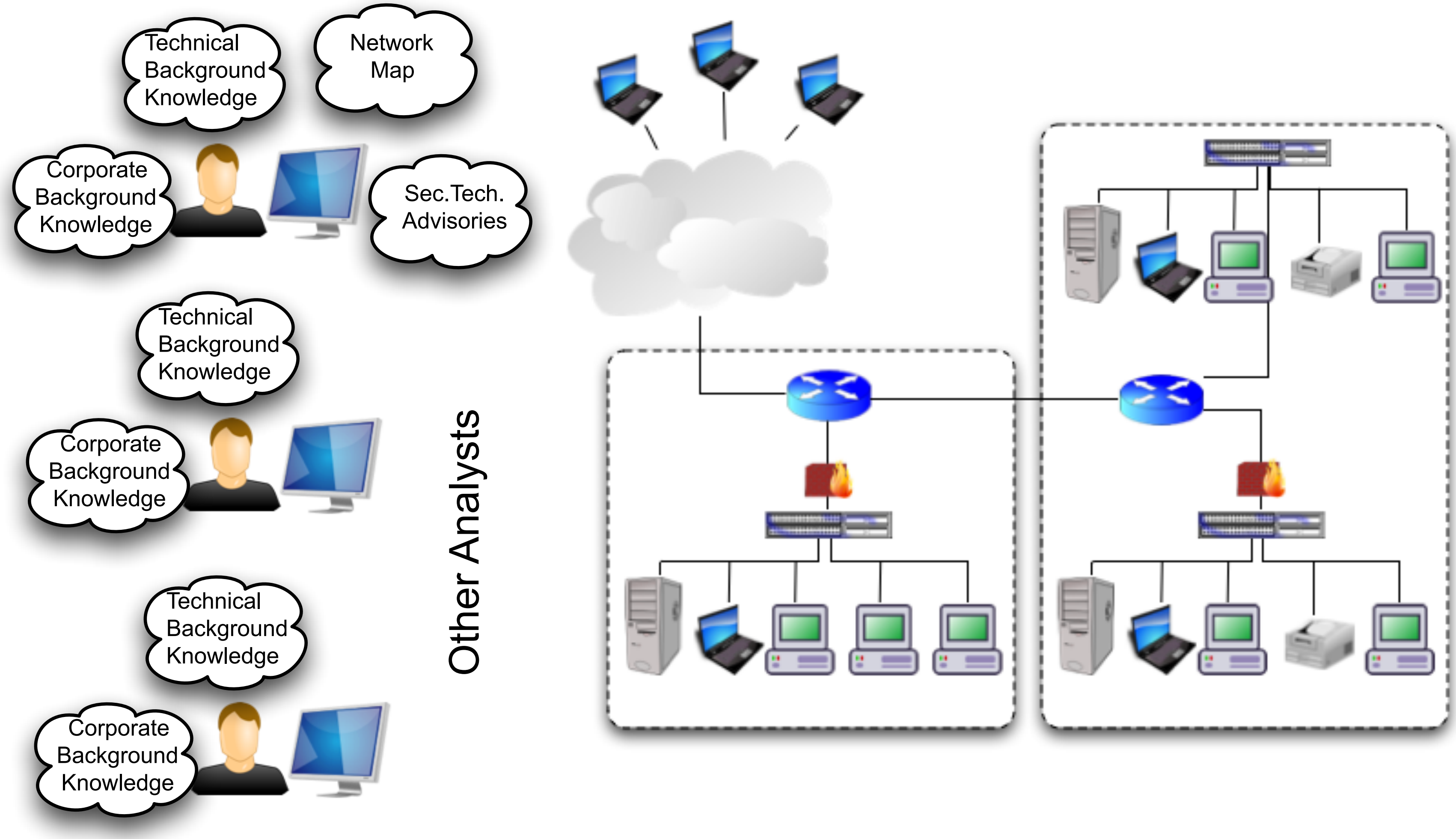
Technical Background Knowledge

Network Map

Corporate Background Knowledge

Sec.Tech. Advisories

Enterprise Network Security



Technical Background Knowledge

Network Map

Corporate Background Knowledge

Sec.Tech. Advisories

Technical Background Knowledge

Corporate Background Knowledge

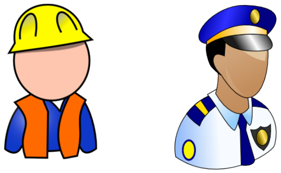
Technical Background Knowledge

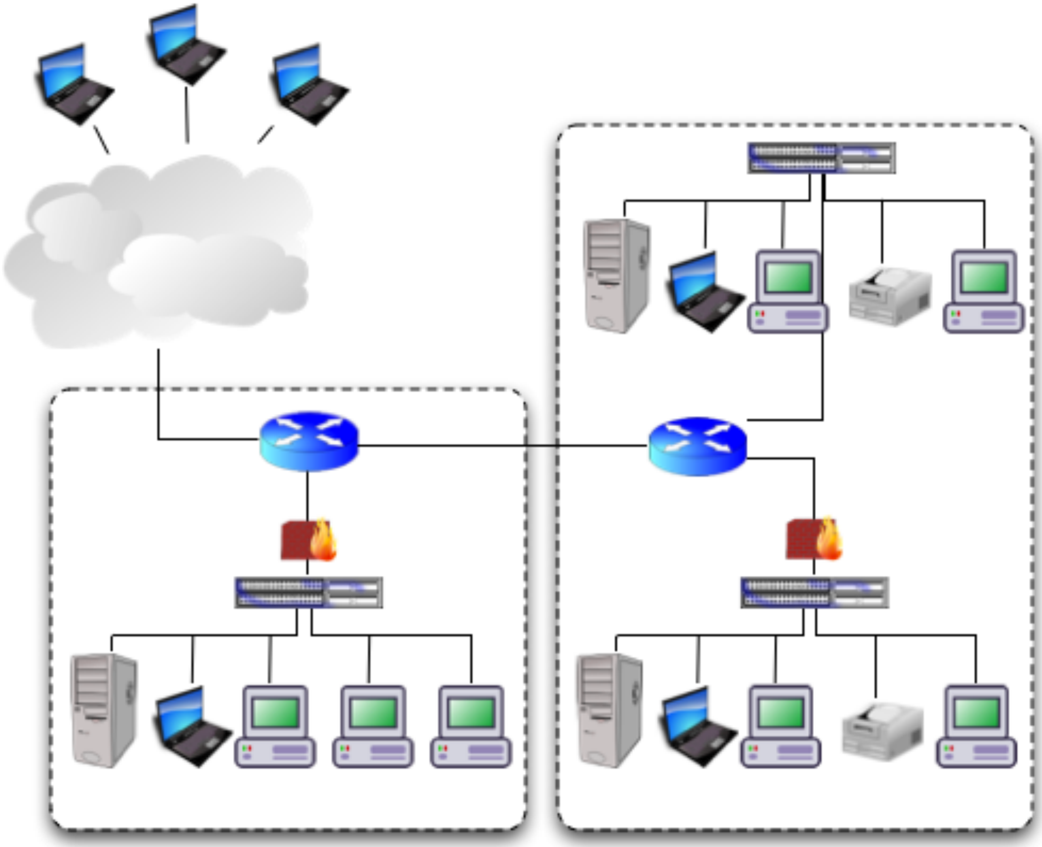
Corporate Background Knowledge

Other Analysts

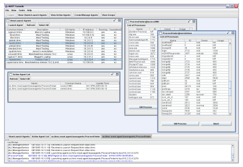
Proposed Approach

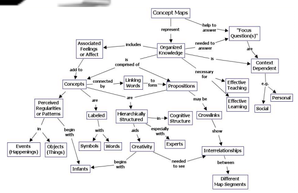
- Shared Knowledge Models between analysts
- Autonomous Software Agents acting as roaming security guards
  - Better Coverage and enforcement of security policies
  - Disconnected Operation
  - Cognitive Software Agents for Analyst support
  - Specialized Agents for Security and Network Discovery





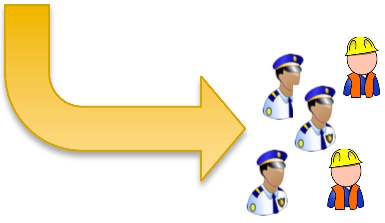
Enterprise Network Security

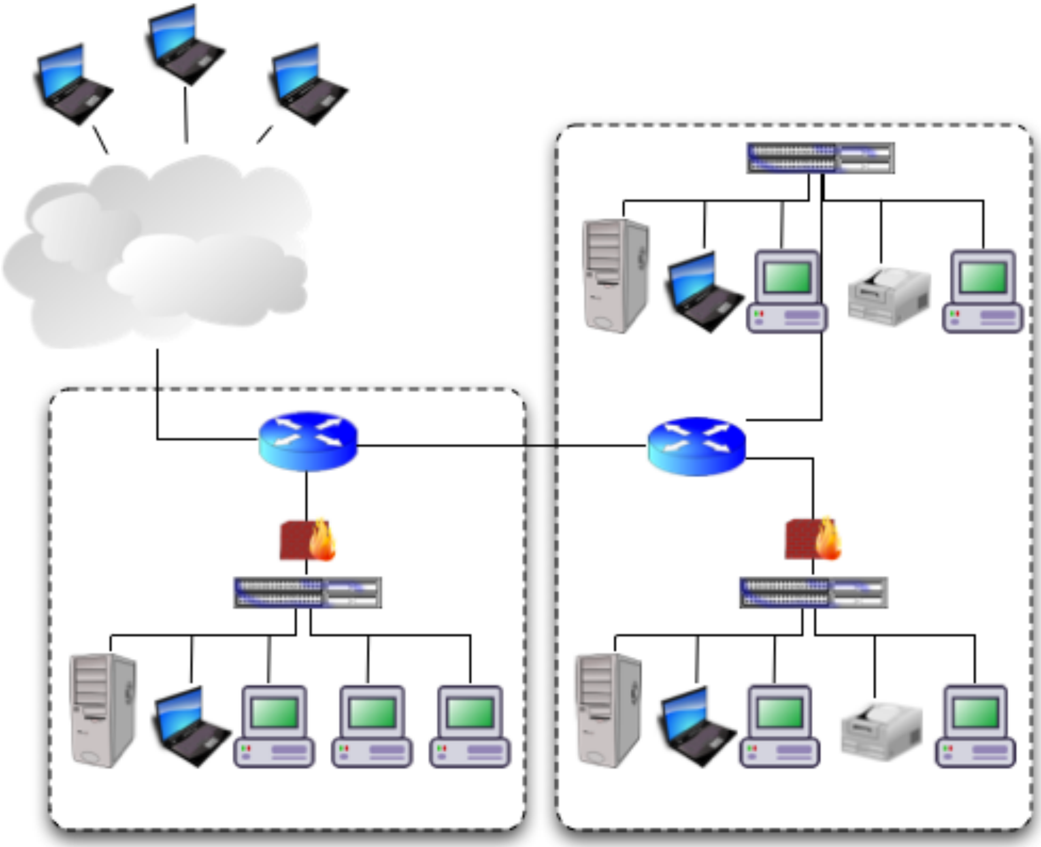




Agent Management

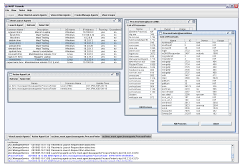
Knowledge Management



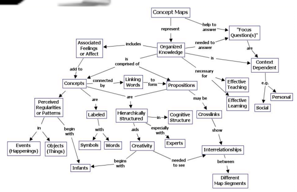


Marco Carvallho (mcarvalho@ihmc.us)

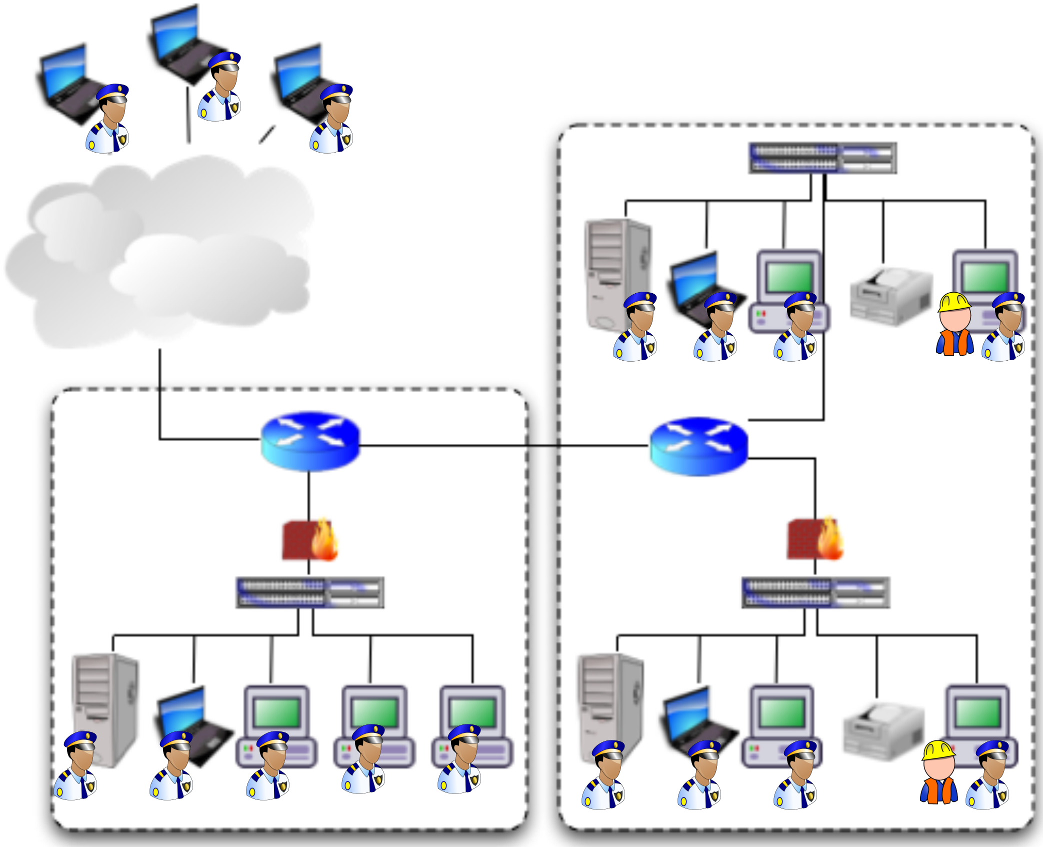
Enterprise Network Security



Agent Management

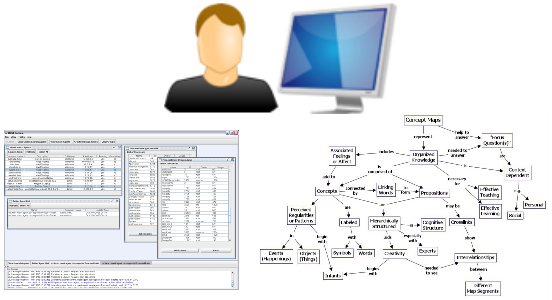


Knowledge Management



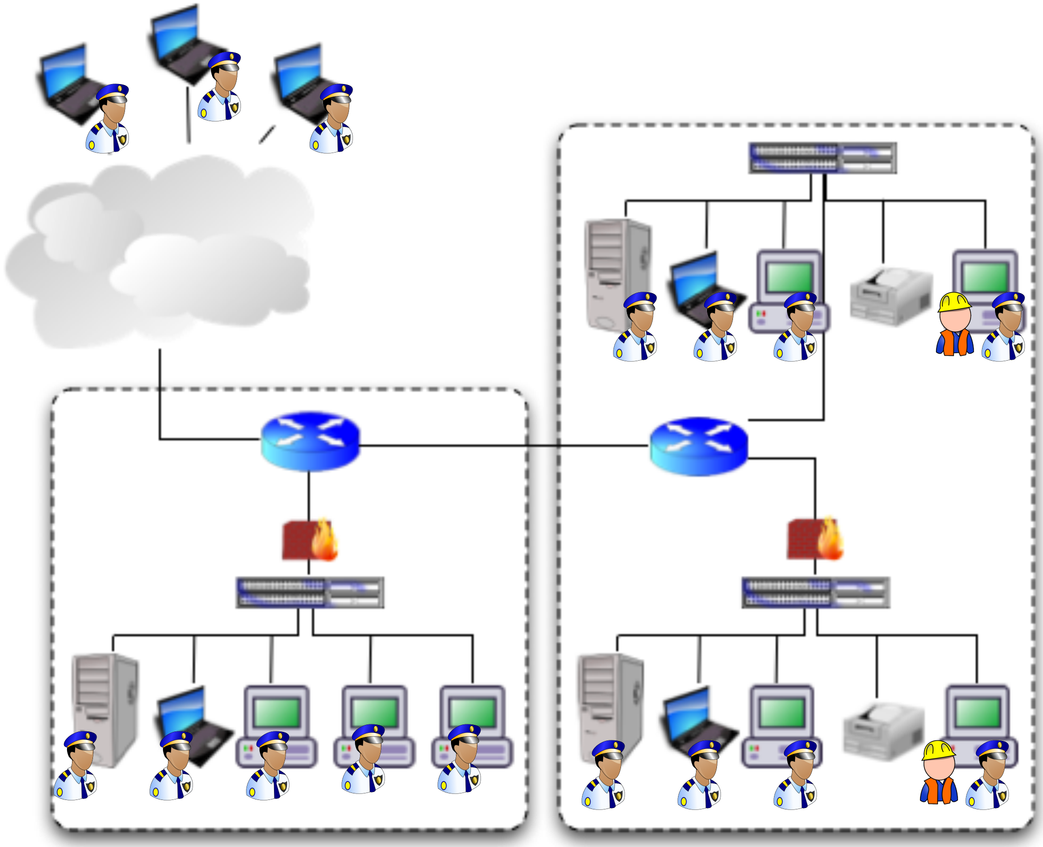
Marco Carvallho (mcarvalho@ihmc.us)

Enterprise Network Security



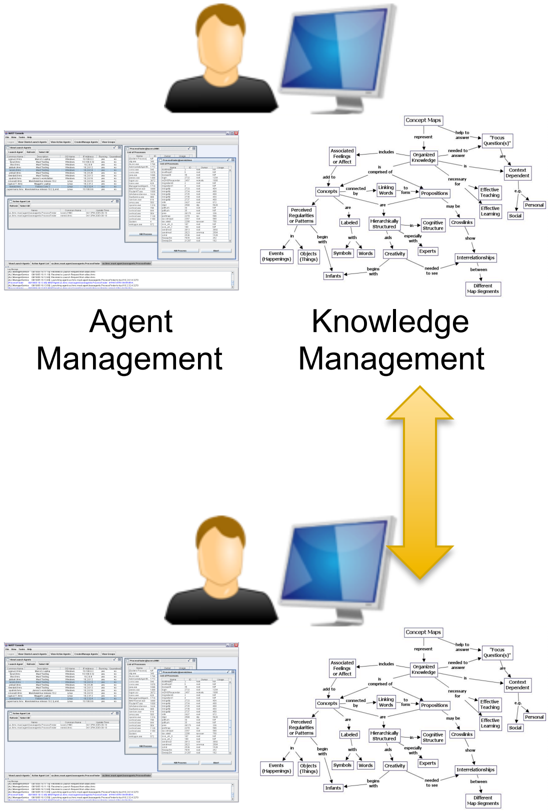
Agent Management

Knowledge Management



- □ Mediating knowledge representation between humans
- □ Graphical notation using concepts, links, and attached resources
- □ NOT a formal representation like a conceptual graph or a semantic network
- □ Flexible and easy-to-use metaphor for expressing and browsing knowledge

Enterprise Network Security

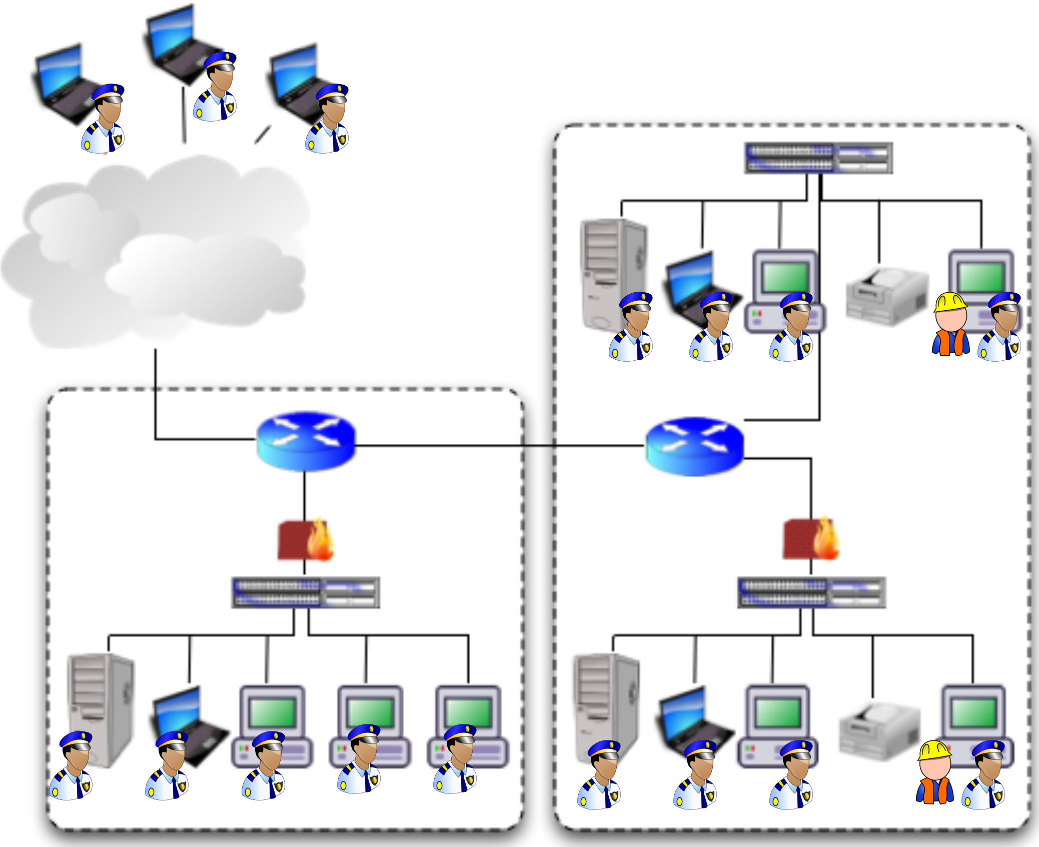


Agent Management

Knowledge Management

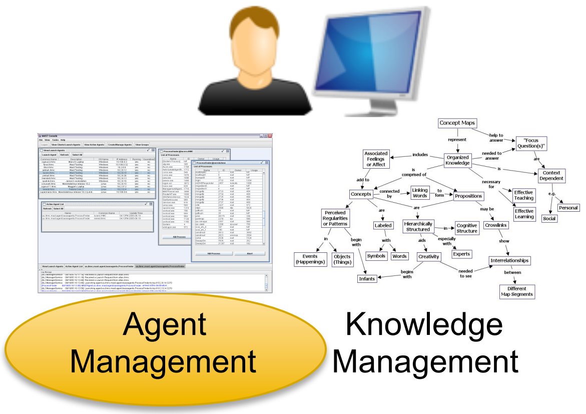
Agent Management

Knowledge Management



Marco Carvallho (mcarvalho@ihmc.us)

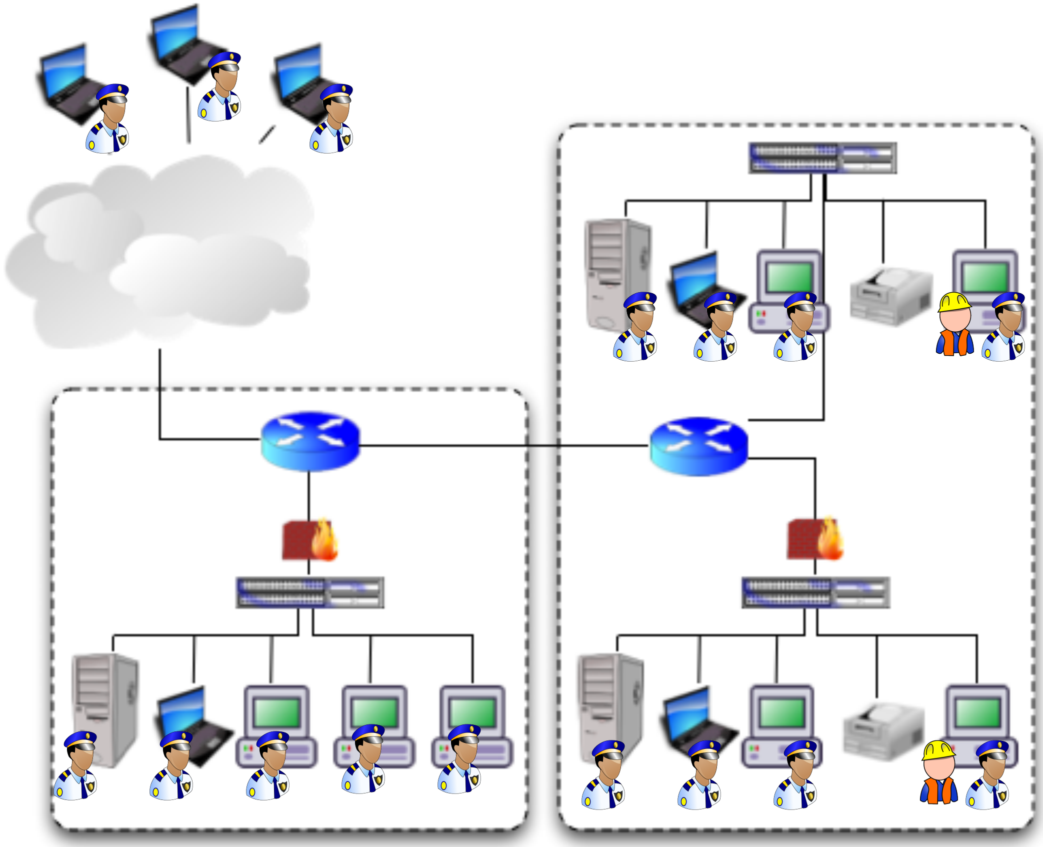
Enterprise Network Security



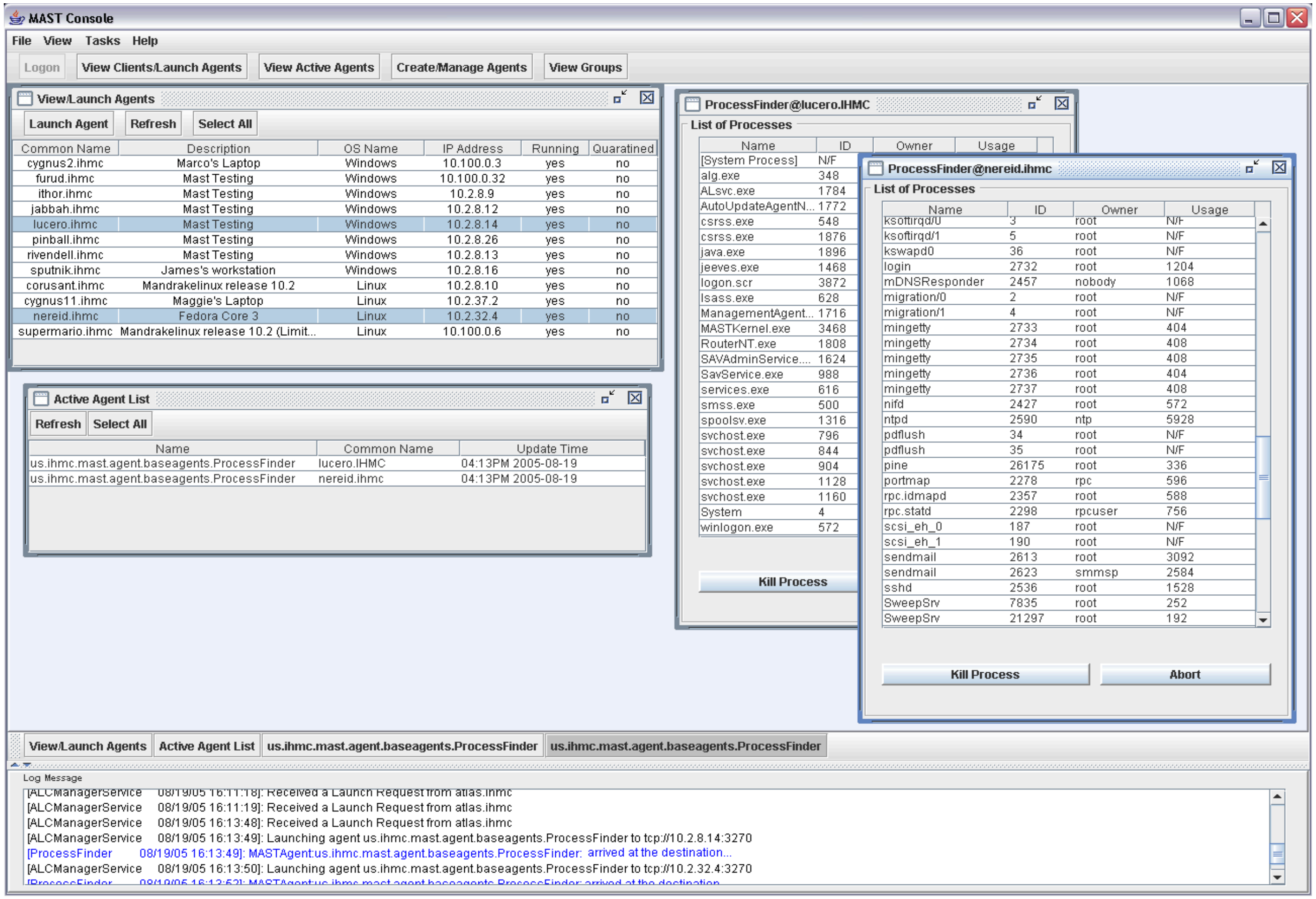
Agent Management

Knowledge Management

- □ Simple security/admin operations
- □ Maintains state across multiple hosts
- □ Ensure system coverage
- □ Supports disconnected operations
- □ Multiple perspectives for network discovery
- □ Persistent operations (at shutdown)
- □ Off-site policy enforcement



The Agent Management Console



Common Name	Description	OS Name	IP Address	Running	Quaratined
cygnus2.ihmc	Marco's Laptop	Windows	10.100.0.3	yes	no
furud.ihmc	Mast Testing	Windows	10.100.0.32	yes	no
ithor.ihmc	Mast Testing	Windows	10.2.8.9	yes	no
jabbah.ihmc	Mast Testing	Windows	10.2.8.12	yes	no
lucero.ihmc	Mast Testing	Windows	10.2.8.14	yes	no
pinball.ihmc	Mast Testing	Windows	10.2.8.26	yes	no
rivendell.ihmc	Mast Testing	Windows	10.2.8.13	yes	no
sputnik.ihmc	James's workstation	Windows	10.2.8.16	yes	no
corusant.ihmc	Mandrakelinux release 10.2	Linux	10.2.8.10	yes	no
cygnus11.ihmc	Maggie's Laptop	Linux	10.2.37.2	yes	no
nereid.ihmc	Fedora Core 3	Linux	10.2.32.4	yes	no
supermario.ihmc	Mandrakelinux release 10.2 (Limit...	Linux	10.100.0.6	yes	no

Active Agent List

Name	Common Name	Update Time
us.ihmc.mast.agent.baseagents.ProcessFinder	lucero.IHMC	04:13PM 2005-08-19
us.ihmc.mast.agent.baseagents.ProcessFinder	nereid.ihmc	04:13PM 2005-08-19

ProcessFinder@lucero.IHMC

List of Processes

Name	ID	Owner	Usage
[System Process]	N/F		
alg.exe	348		
ALsvc.exe	1784		
AutoUpdateAgentN...	1772		
csrss.exe	548		
csrss.exe	1876		
java.exe	1896		
jeeves.exe	1468		
logon.scr	3872		
lsass.exe	628		
ManagementAgent...	1716		
MASTKernel.exe	3468		
RouterNT.exe	1808		
SAVAdminService....	1624		
SavService.exe	988		
services.exe	616		
smss.exe	500		
spoolsv.exe	1316		
svchost.exe	796		
svchost.exe	844		
svchost.exe	904		
svchost.exe	1128		
svchost.exe	1160		
System	4		
winlogon.exe	572		

ProcessFinder@nereid.ihmc

List of Processes

Name	ID	Owner	Usage
ksoftirqd/0	3	root	N/F
ksoftirqd/1	5	root	N/F
kswapd0	36	root	N/F
login	2732	root	1204
mDNSResponder	2457	nobody	1068
migration/0	2	root	N/F
migration/1	4	root	N/F
mingetty	2733	root	404
mingetty	2734	root	408
mingetty	2735	root	408
mingetty	2736	root	404
mingetty	2737	root	408
nifd	2427	root	572
ntpd	2590	ntp	5928
pdflush	34	root	N/F
pdflush	35	root	N/F
pine	26175	root	336
portmap	2278	rpc	596
rpc.idmapd	2357	root	588
rpc.statd	2298	rpcuser	756
scsi_eh_0	187	root	N/F
scsi_eh_1	190	root	N/F
sendmail	2613	root	3092
sendmail	2623	smmsp	2584
sshd	2536	root	1528
SweepSrv	7835	root	252
SweepSrv	21297	root	192

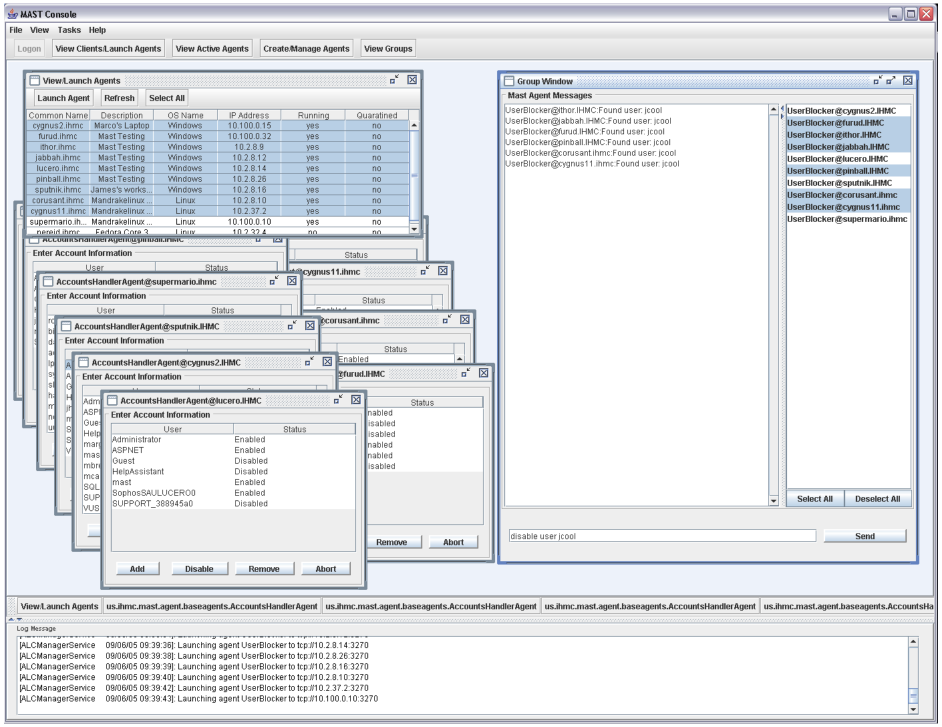
```
[ALCManagerService    08/19/05 16:11:18]: Received a Launch Request from atlas.ihmc
[ALCManagerService    08/19/05 16:11:19]: Received a Launch Request from atlas.ihmc
[ALCManagerService    08/19/05 16:13:48]: Received a Launch Request from atlas.ihmc
[ALCManagerService    08/19/05 16:13:49]: Launching agent us.ihmc.mast.agent.baseagents.ProcessFinder to tcp://10.2.8.14:3270
[ProcessFinder        08/19/05 16:13:49]: MASTAgent:us.ihmc.mast.agent.baseagents.ProcessFinder:  arrived at the destination...
[ALCManagerService    08/19/05 16:13:50]: Launching agent us.ihmc.mast.agent.baseagents.ProcessFinder to tcp://10.2.32.4:3270
[ProcessFinder        08/19/05 16:13:52]: MASTAgent:us.ihmc.mast.agent.baseagents.ProcessFinder: arrived at the destination...
```

mast.ihmc.us

Lessons Learned

- Building Agents
  - System required the user to explicitly specify the functions of the agent (with few exceptions)
  - Upfront investment for agent creation/customization
- Managing Agents
  - Locating/understanding and launching agents
- Interfacing with Agents
  - Large volume (overload)
  - Difficult to Identify

Attaching Agents to Knowledge Models
Building Chat Interfaces



MAST Console

Common Name	Description	OS Name	IP Address	Running	Quaratined
cygnus2.ihmc	Marco's Laptop	Windows	10.100.0.15	yes	no
furud.ihmc	Mast Testing	Windows	10.100.0.32	yes	no
ithor.ihmc	Mast Testing	Windows	10.2.8.9	yes	no
jabbah.ihmc	Mast Testing	Windows	10.2.8.12	yes	no
lucero.ihmc	Mast Testing	Windows	10.2.8.14	yes	no
pinball.ihmc	Mast Testing	Windows	10.2.8.26	yes	no
sputnik.ihmc	James's works...	Windows	10.2.8.16	yes	no
corusant.ihmc	Mandrakelinux ...	Linux	10.2.8.10	yes	no
cygnus11.ihmc	Mandrakelinux ...	Linux	10.2.37.2	yes	no
supermario.ih...	Mandrakelinux ...	Linux	10.100.0.10	yes	no
nereid.ihmc	Fedora Core 3	Linux	10.2.32.4	no	no

AccountsHandlerAgent@pinball.IHMC

AccountsHandlerAgent@supermario.ihmc

AccountsHandlerAgent@sputnik.IHMC

AccountsHandlerAgent@cygnus2.IHMC

...@cygnus11.ihmc

...@corusant.ihmc

...@furud.IHMC

AccountsHandlerAgent@lucero.IHMC

Enter Account Information

User	Status
Administrator	Enabled
ASPNET	Enabled
Guest	Disabled
HelpAssistant	Disabled
mast	Enabled
SophosSAULUCERO0	Enabled
SUPPORT_388945a0	Disabled

Group Window

Mast Agent Messages

```
UserBlocker@ithor.IHMC:Found user: jcool
UserBlocker@jabbah.IHMC:Found user: jcool
UserBlocker@furud.IHMC:Found user: jcool
UserBlocker@pinball.IHMC:Found user: jcool
UserBlocker@corusant.ihmc:Found user: jcool
UserBlocker@cygnus11.ihmc:Found user: jcool
```

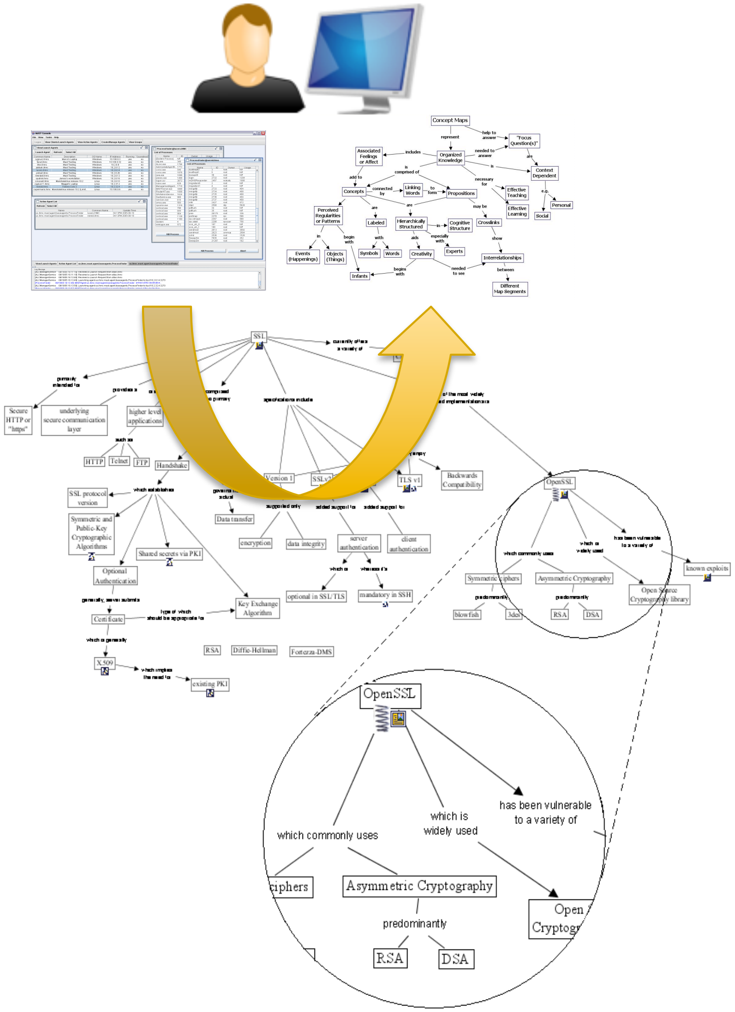
UserBlocker@cygnus2.IHMC
UserBlocker@furud.IHMC
UserBlocker@ithor.IHMC
UserBlocker@jabbah.IHMC
UserBlocker@lucero.IHMC
UserBlocker@pinball.IHMC
UserBlocker@sputnik.IHMC
UserBlocker@corusant.ihmc
UserBlocker@cygnus11.ihmc
UserBlocker@supermario.ihmc

disable user jcool

Send
View/Launch Agents
us.ihmc.mast.agent.baseagents.AccountsHandlerAgent
us.ihmc.mast.agent.baseagents.AccountsHandlerAgent
us.ihmc.mast.agent.baseagents.AccountsHandlerAgent
us.ihmc.mast.agent.baseagents.AccountsHa

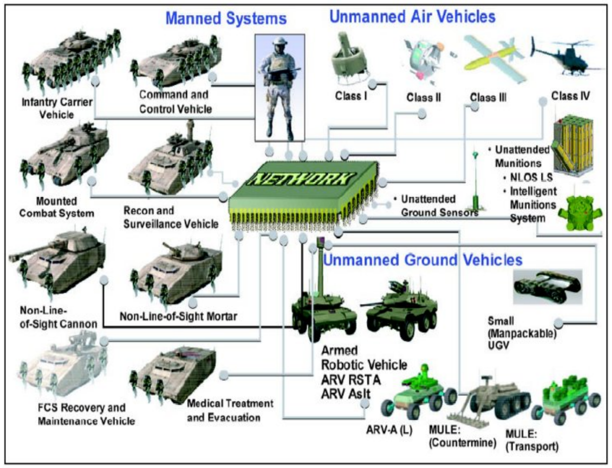
Log Message

```
[ALCManagerService    09/06/05 09:39:36]: Launching agent UserBlocker to tcp://10.2.8.14:3270
[ALCManagerService    09/06/05 09:39:38]: Launching agent UserBlocker to tcp://10.2.8.26:3270
[ALCManagerService    09/06/05 09:39:39]: Launching agent UserBlocker to tcp://10.2.8.16:3270
[ALCManagerService    09/06/05 09:39:40]: Launching agent UserBlocker to tcp://10.2.8.10:3270
[ALCManagerService    09/06/05 09:39:42]: Launching agent UserBlocker to tcp://10.2.37.2:3270
[ALCManagerService    09/06/05 09:39:43]: Launching agent UserBlocker to tcp://10.100.0.10:3270
```



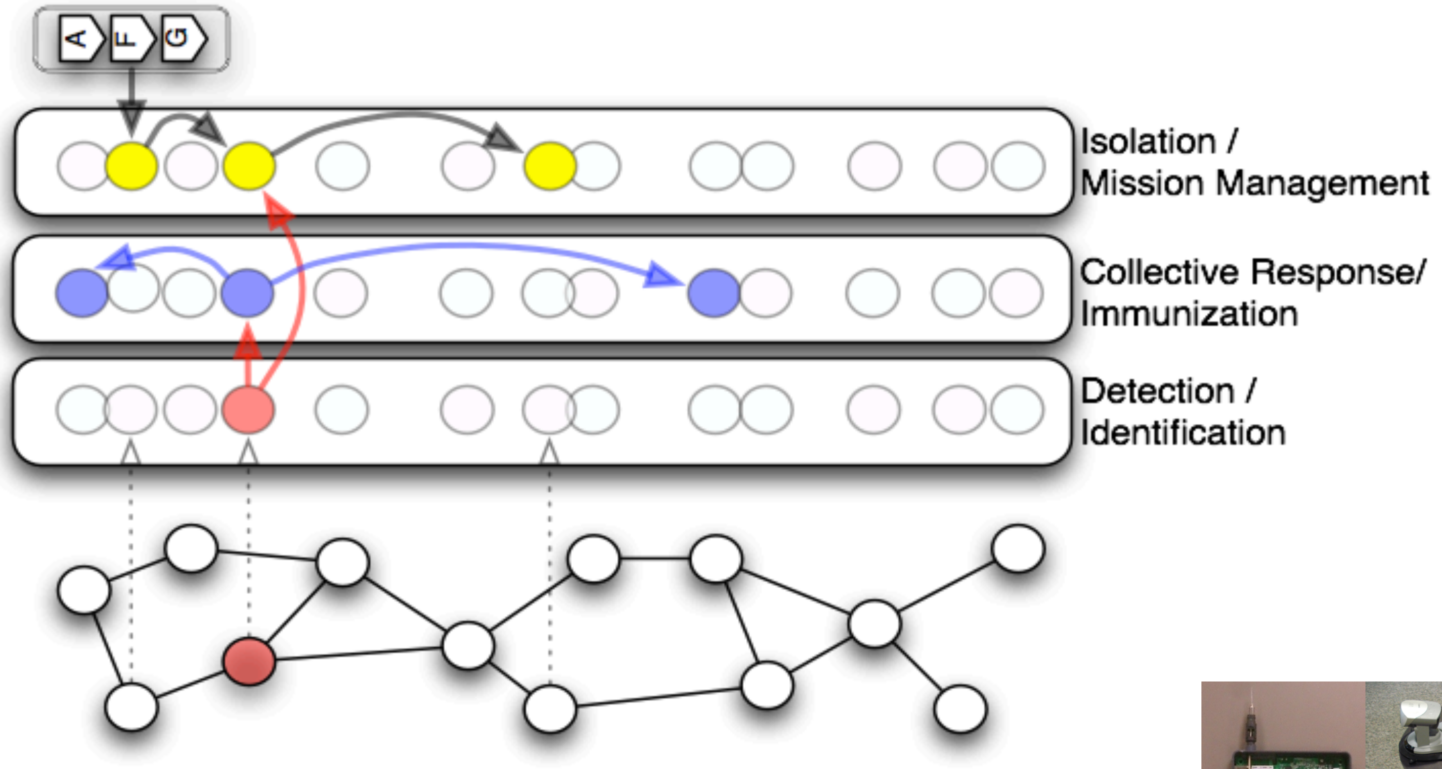
mast.ihmc.us

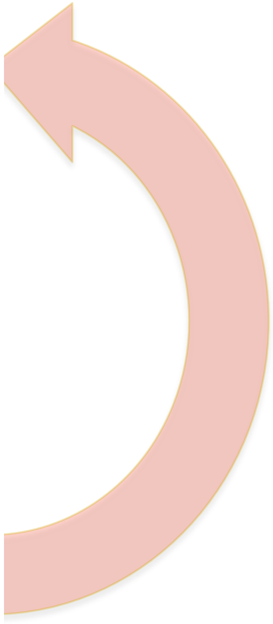
Biologically Inspired Tactical Security Infrastructure
(Army Research Laboratory)

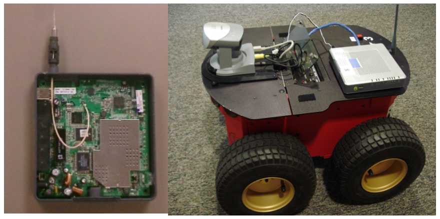


- Sponsor: Army Research Laboratory
- Collaborative Project with the Florida Institute of Technology
- Enabling Mission Survivability – “Fighting Through” Capabilities)

Proof-of-Concept Implementation: Mission Survivability

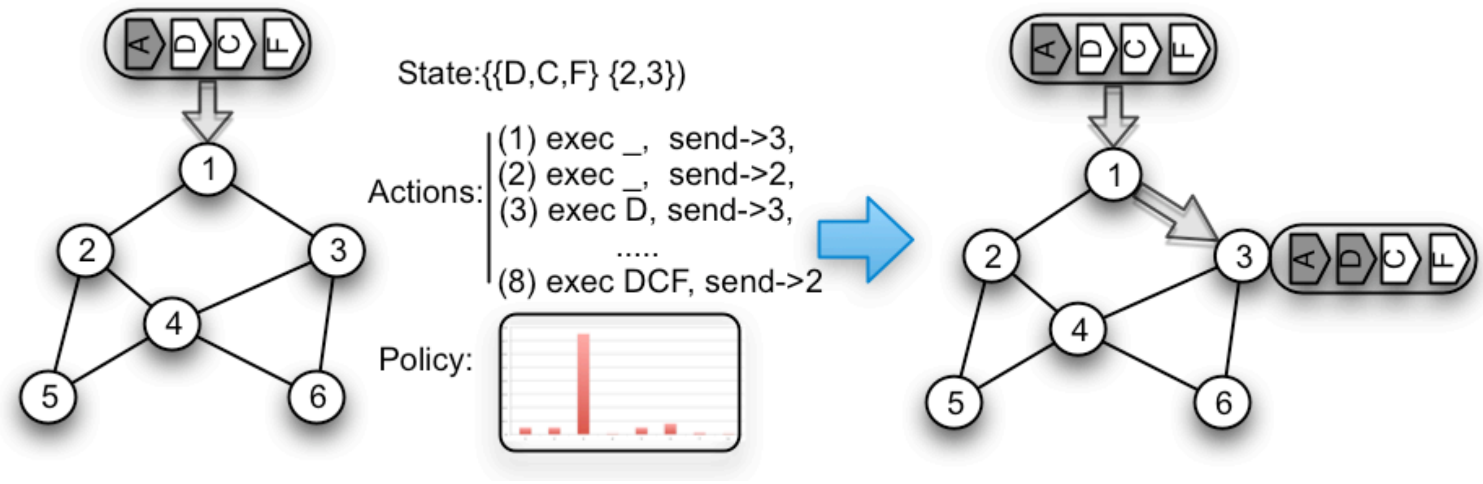

A
F
G
Isolation / Mission Management
Collective Response/ Immunization
Detection / Identification





- Maintain System operations in face of disruptions
- Reactive and proactive reconfiguration for mission continuity (slow the high-freq. effects)

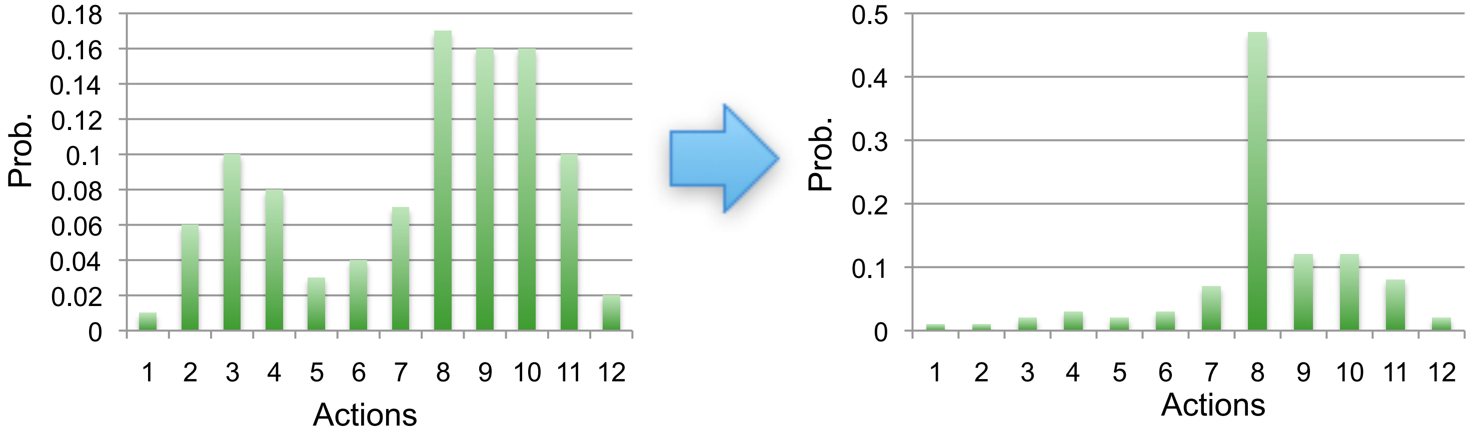
Policy Estimation



State:{{D,C,F} {2,3})

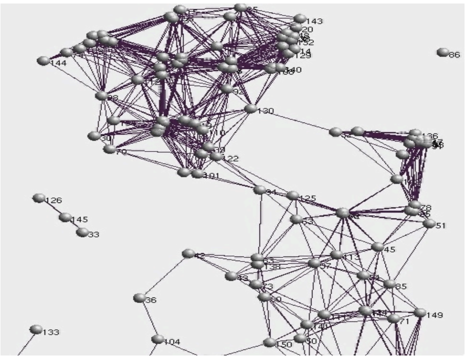
Actions:
(1) exec _, send->3,
(2) exec _, send->2,
(3) exec D, send->3,
.....
(8) exec DCF, send->2

Policy:



Lessons Learned

- Understanding the environment
  - Dynamics of the system
  - Dynamics of the defense infrastructure
- Eventual dissonance between user’s mental models and collective agent responses (poor mission mapping)
- Benefits in slowing down high-frequency effects for human response (engine failure at take-off example)



• Maintain System operations in face of disruptions
• Reactive and proactive reconfiguration for mission continuity (slow the high-freq. effects)

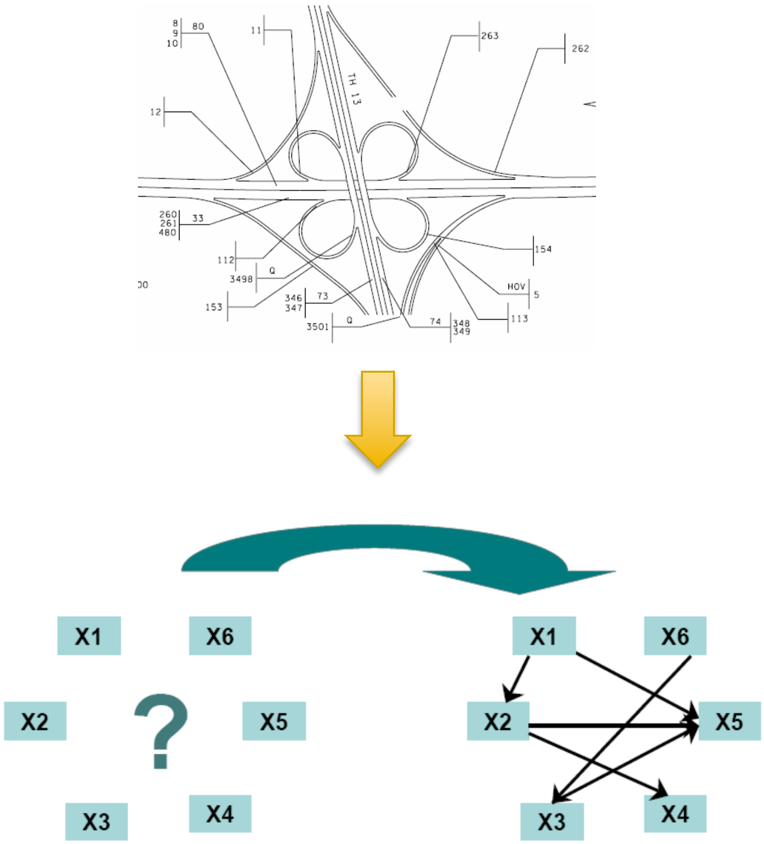
Traffic Management

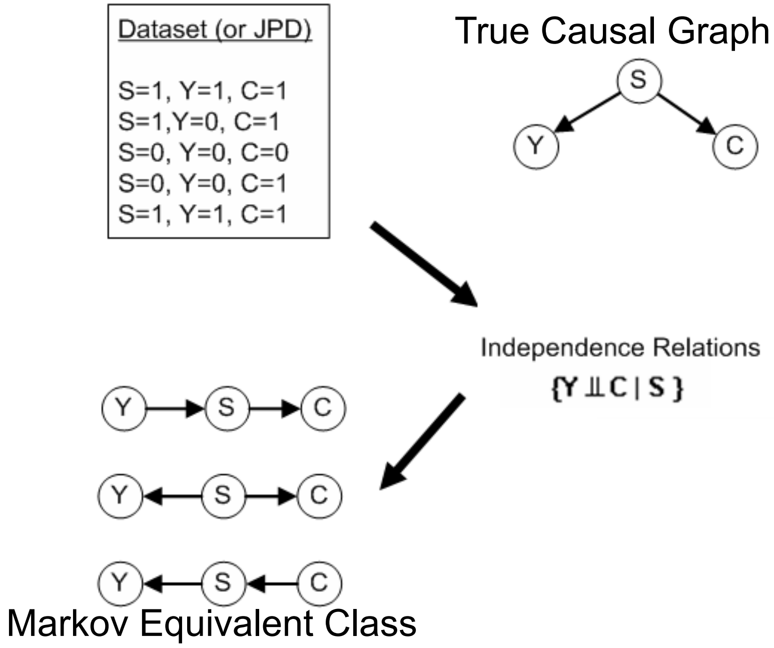
- Monitored by operators in centralized control centers
  - Mostly used for traffic announcements and dispatches
  - Thousands of data collection sensors (indirect measurements)
  - MnDOT (54K Twin Cities Metro)

- Problem: Understand the interdependencies of the system (spatial/temporal) for corrective/preventive action
  (Greatly relies on user expertise)

Transportation Systems

Automatic Regulatory Structure Discovery for Accident Prevention





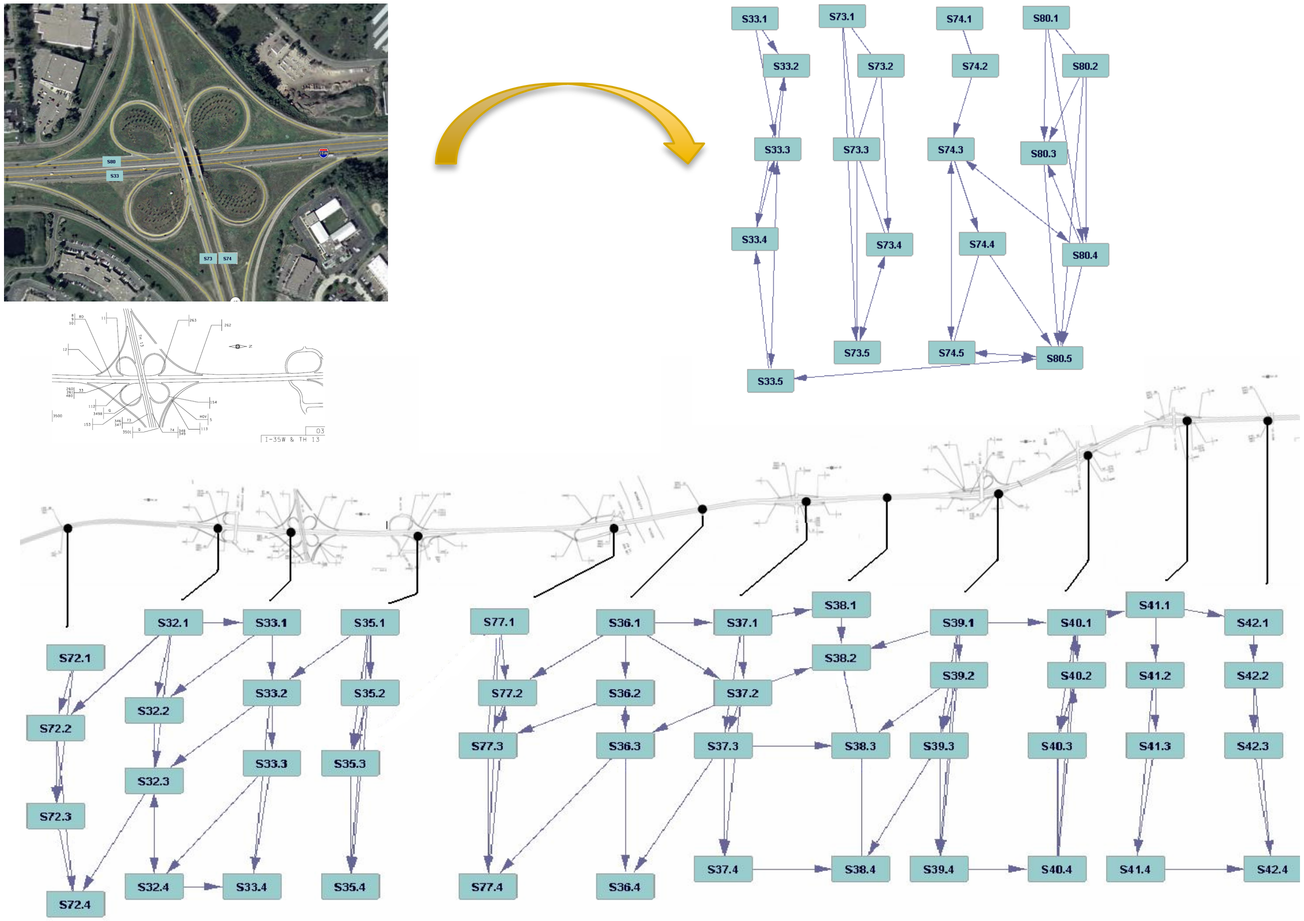
Dataset (or JPD)

S=1, Y=1, C=1
S=1,Y=0, C=1
S=0, Y=0, C=0
S=0, Y=0, C=1
S=1, Y=1, C=1

Marco Carvallho (mcarvalho@ihmc.us)

Transportation Systems

Automatic Regulatory Structure Discovery for Accident Prevention

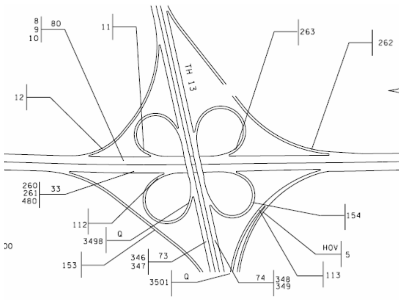


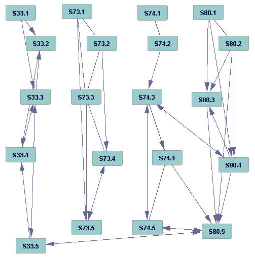
Marco Carvallho (mcarvalho@ihmc.us)

Lessons Learned

- Powerful in providing some insight on useful knobs
  - Often known by experienced operators
- Lack of projection (what if) capabilities
- Structure discovery process is obscure at times
  - Lack of trust in the process

Minneapolis
Roseville
Falcon Heights
Lauderdale
St Louis Park
Uptown
CARAG
Prospect Park
Cooper
Ericsson
Edina
Mendota
Mendota Heights
Lilydale
Minneapolis-Saint Paul International Airport
Atwood





Lessons Learned

- It is more than just a visualization issue (although visualization is very important)
- Understanding the *collective* actions and effects of individual agents
- Tracking and predicting the trajectory of the system
- Tracking the progress of Agents (Progress Appraisal)
- It is about teamwork!
  - Collaborative environment
  - Policy regulation
  - Learning from experience

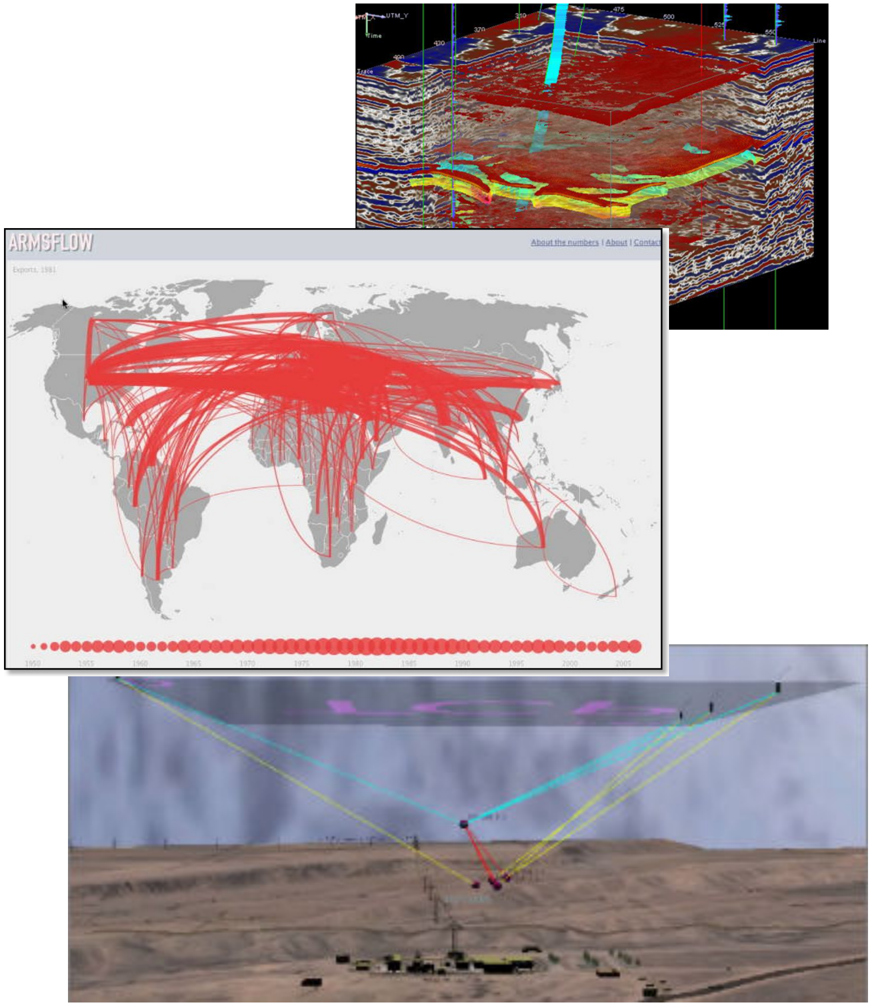
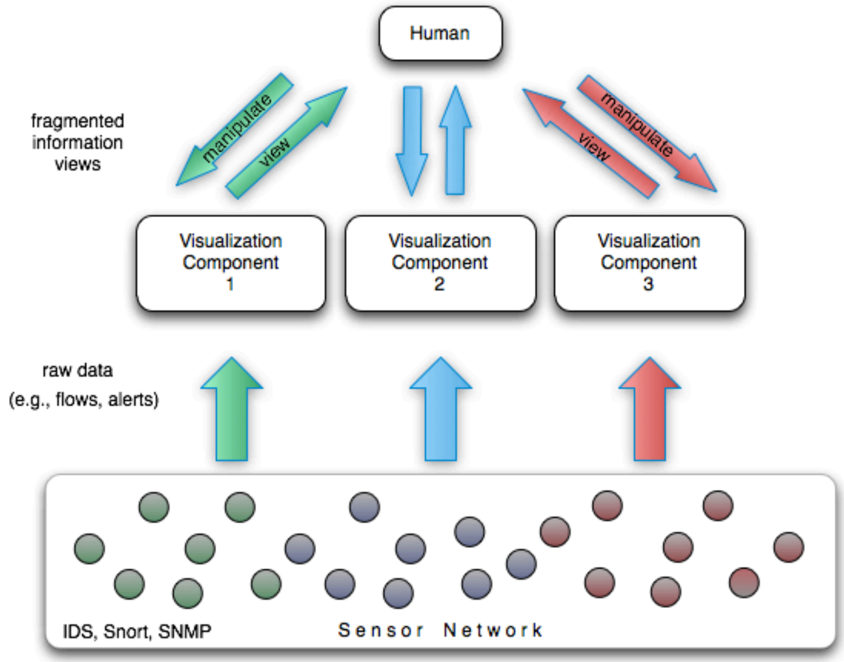


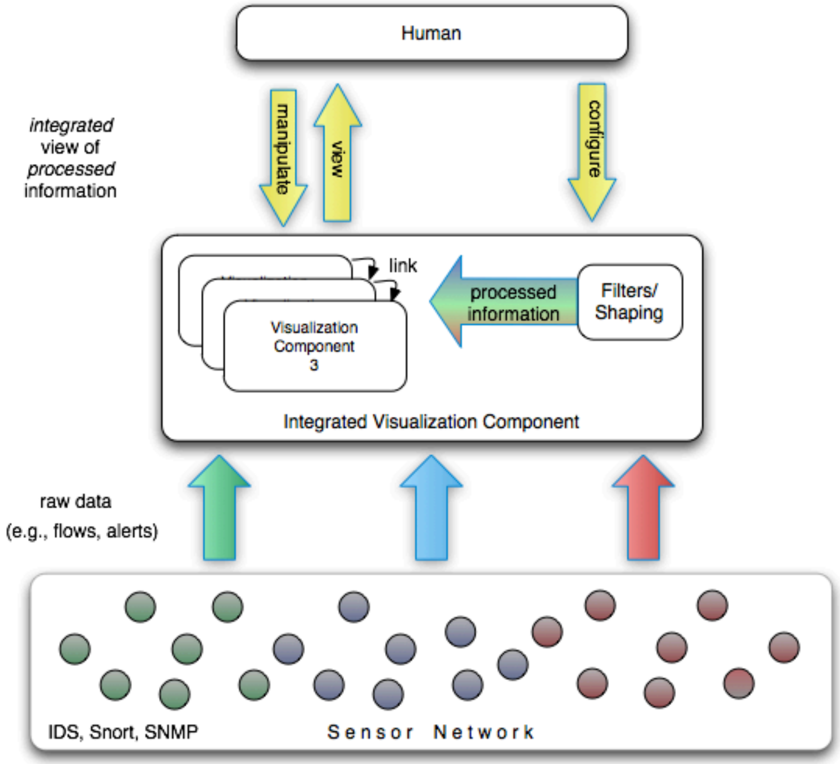
Image Source: Sandia, cyber3D Informatique,armsflow

Ongoing Developments


Human
fragmented information views
manipulate
view
view
manipulate
Visualization Component 1
Visualization Component 2
Visualization Component 3
raw data (e.g., flows, alerts)
IDS, Snort, SNMP
Sensor Network

- Separate Interfaces to different views of system
  - Human is responsible for maintaining the mental model of the systems
  - Advanced filters help improve the understanding of each perspective
  - Mission Goals exist only at human level

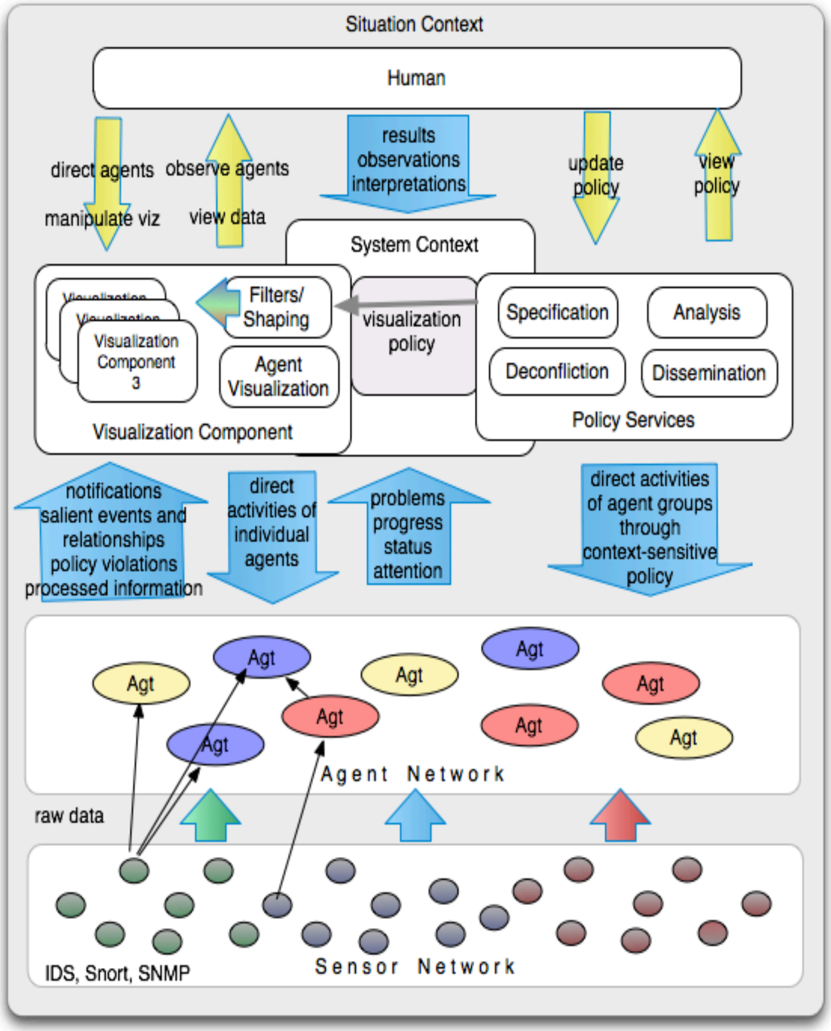
Ongoing Developments


Human
integrated view of processed information
manipulate
view
configure
link
Visualization Component 3
processed information
Filters/ Shaping
Integrated Visualization Component
raw data (e.g., flows, alerts)
IDS, Snort, SNMP
Sensor Network

- Information Fusion
  - Fusing multiple sources of data or perspectives in a common view
  - Focus on visualization technologies
  - Automatic data analysis may identify correlations between events and sources
  - Mission goals still reside at the human level
  - Filter/Fusion definition is done offline – for the optimization of pre-defined tasks

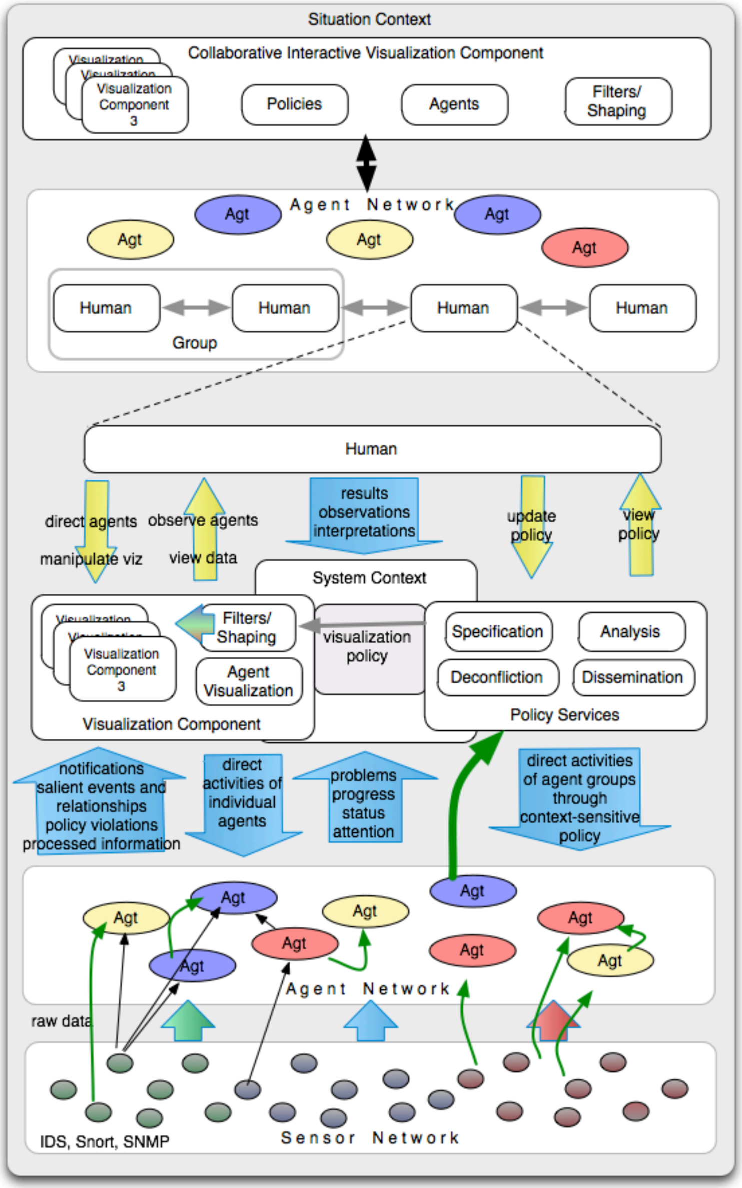
IHMC Cyber SA Framework

- Policy-based multi-agent system for teamwork support
- Data Processing Agents
  - Simple Data Processing for data filtering
  - Pre-defined pattern search
  - Self Organizing hierarchies
  - Template hierarchies for specific tasks (created/ accepted)
  - Randomized Patterns Search
  - Explicit user feedback
    - Through policies and configuration
  - Implicit user feedback
    - Visualization controls



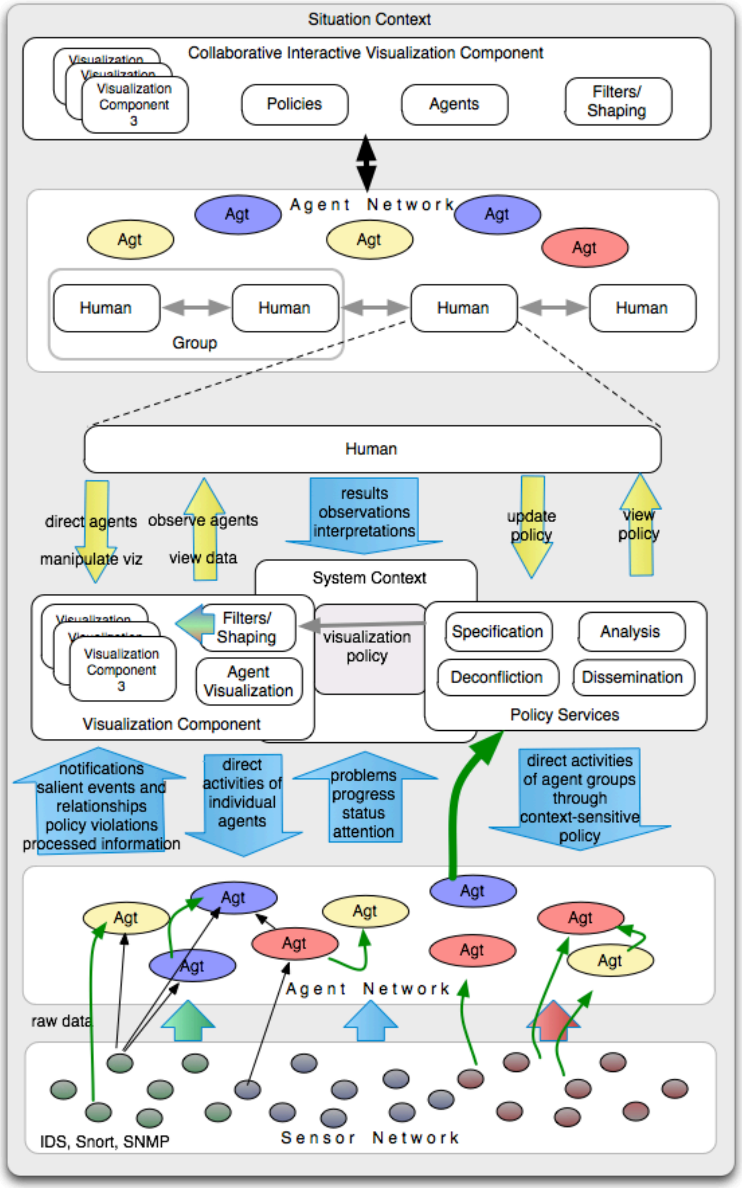
Cognitive Software Agents

- Multi-user collaborative environment
- Cognitive Agents
  - Collect information from multiple agents/sources
  - Learn from human actions and explicit procedural descriptions
  - Build hypothesis based on sequence of events
    - Branch parallel test for validation/ negation
  - Learn new system policies through task refinement

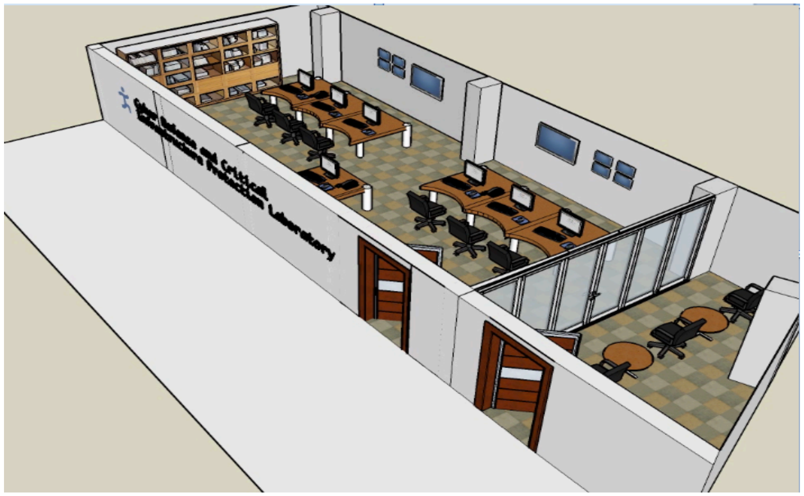


Cognitive Software Agents

- Agent functionality is represented in an ontology (using OWL).
- Analysts can assemble agents to create workflows at runtime.
- Mechanism for knowledge Capture (sharing)
- Agents publish their capabilities (functional descriptions) – other agents can assemble flows automatically (self-organization)
- Data-driven model for flow tasking and organization



Current Application:
Cyber Defense Situation Awareness


Cyber Defense and Critical
Infrastructure Protection Laboratory

Sponsor: DoD and Industry
Mixed-Initiative Multi-Agent Systems
for Cyber Situation Awareness

CyberLab (Ocala, FL)

Acknowledgements

Cyber Situation Awareness

- Jeff Bradshaw
- Larry Bunch
- Tom Eskridge
- Paul Feltovitch
- Matt Johnson

Cyber Lab

- Carlos Perez
- Adrian Granados
- Marco Arguedas
- Massimiliano Marcon
- Giacomo Benincasa

Thank you!

Marco Carvalho
Research Scientist
mcarvalho@ihmc.us
(850) 202-4446

Institute for Human and Machine Cognition
15 SE Osceola Ave.
Ocala, FL.

www.ihmc.us